

ABSTRACT

Practical Application of PRA as an Integrated Design Tool for Space Systems

By: Prince Kalia, Ying Shi, Robin Pair, Virginia Quaney and John Uhlenbrock

This paper presents the application of the first comprehensive Probabilistic Risk Assessment (PRA) during the design phase of a joint NASA/NOAA weather satellite program, Geostationary Operational Environmental Satellite Series R (GOES-R). GOES-R is the next generation weather satellite primarily to help understand the weather and help save human lives. PRA has been used at NASA for Human Space Flight for many years. PRA was initially adopted and implemented in the operational phase of manned space flight programs and more recently for the next generation human space systems. Since its first use at NASA, PRA has become recognized throughout the Agency as a method of assessing complex mission risks as part of an overall approach to assuring safety and mission success throughout project lifecycles. PRA is now included as a requirement during the design phase of both NASA next generation manned space vehicles as well as for high priority robotic missions. The influence of PRA on GOES-R design and operation concepts are discussed in detail.

The GOES-R PRA is unique at NASA for its early implementation. It also represents a pioneering effort to integrate risks from both Spacecraft (SC) and Ground Segment (GS) to fully assess the probability of achieving mission objectives. PRA analysts were actively involved in system engineering and design engineering to ensure that a comprehensive set of technical risks were correctly identified and properly understood from a design and operations perspective. The analysis included an assessment of SC hardware and software, SC fault management system, GS hardware and software, common cause failures, human error, natural hazards, solar weather and infrastructure (such as network and telecommunications failures, fire).

PRA findings directly resulted in design changes to reduce SC risk from micro-meteoroids. PRA results also led to design changes in several SC subsystems, e.g. propulsion, guidance, navigation and control (GNC), communications, mechanisms, and command and data handling (C&DH). The fault tree approach assisted in the development of the fault management system design. Human error analysis, which examined human response to failure, indicated areas where automation could reduce the overall probability of gaps in operation by half. In addition, the PRA brought to light many potential root causes of system disruptions, including earthquakes, inclement weather, solar storms, blackouts and other extreme conditions not considered in the typical reliability and availability analyses. Ultimately the PRA served to identify potential failures that, when mitigated, resulted in a more robust design, as well as to influence the program's concept of operations. The early and active integration of PRA with system and design engineering provided a well-managed approach for risk assessment that increased reliability and availability, optimized lifecycle costs, and unified the SC and GS developments.